(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2000163376 A

(43) Date of publication of application: 16.06.00

(51) Int. Cl G06F 15/00
H04L 9/32
H04L 12/14

(21) Application number: 10375506

(22) Date of filing: 27.11.98

(71) Applicant: OKUMURA TAKASHI

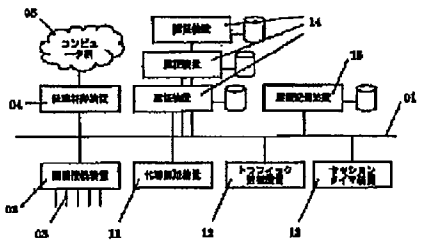
(72) Inventor: OKUMURA TAKASHI

(54) COMPUTER NETWORK COMMUNICATION CERTIFICATE AND HISTORY RECORDING DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To enable charging corresponding to the style of utilization by recording communication histories by detecting communication for each combination of user ID and utilization protocol and calculating the length of a session, and utilizing these communication histories.

SOLUTION: By recording the communication history for each combination of user ID and utilization protocol, precise charging corresponding to the communication style of a user is enabled. At the same time, the scale of user certification can be expanded.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－163376
(P2000－163376A)
(43)公開日　平成12年６月16日(2000.6.16)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
G06F	15/00	330	G06F	15/00	330B	5B085
H04L	9/32		H04L	9/00	673A	5J104
	12/14				673Z	5K030
				11/02	F	9A001

審査請求　未請求　請求項の数６　書面　（全 ９ 頁）

(21)出願番号　特願平10－375506

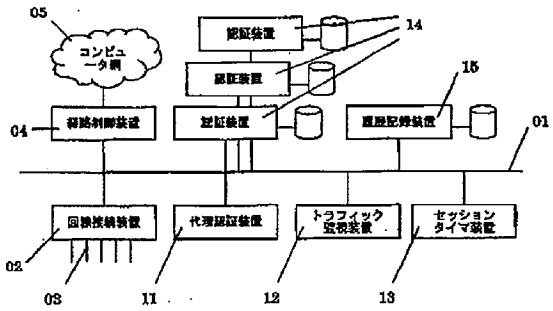
(22)出願日　平成10年11月27日(1998.11.27)

(71)出願人　599002825
奥村　貴史
東京都台東区蔵前３－８－９
(72)発明者　奥村　貴史
東京都台東区蔵前３－８－９

Ｆターム(参考)　5B085 AC04 AC14 AE02 AE23 BG07
5J104 AA07 KA01 KA04 NA05 NA27
NA36 NA38 PA07
5K030 GA15 HB08 HC01 HC13 KA07
MB09
9A001 EE03 LL03

(54)【発明の名称】　コンピュータ網接続認証及び履歴記録装置

(57)【要約】
【課題】従来のダイヤルアップによるコンピュータ網接続における課金においては、送受信データ量や総接続時間に基づいた課金しか可能ではなかった。
【解決手段】本発明は、利用者ＩＤと利用プロトコルの組み合わせ毎に通信履歴を記録することによって、利用者の通信形態に応じた細かな課金を可能とする。同時に、利用者認証の大規模化を可能とする。



1

【特許請求の範囲】

【請求項１】コンピュータ網への接続認証の際に、利用者ＩＤと利用者に割り当てたネットワークアドレスとの対応表を作成する装置と、送受信パケットの中に含まれるネットワークアドレスおよび利用プロトコルを検出するトラフィック監視装置と、該トラフィック監視装置からの通知及び上記対応表によって利用者ＩＤと利用プロトコルの組み合わせ毎に通信時間を計測するタイマによって、利用者ＩＤと利用プロトコルの組み合わせ毎に通信時間の履歴を算出および記録する装置。

【請求項２】コンピュータ網への接続認証の際に、利用者ＩＤと利用者に割り当てたネットワークアドレスとの対応表を作成する方法と、送受信パケットの中に含まれるネットワークアドレスおよび利用プロトコルを検出するトラフィック監視方法と、該トラフィック監視装置からの通知及び上記対応表によって利用者ＩＤと利用プロトコルの組み合わせ毎に通信時間を計測するタイマによって、利用者ＩＤと利用プロトコルの組み合わせ毎に通信時間の履歴を算出および記録する方法。

【請求項３】請求項１、２のコンピュータ網への接続認証において、回線接続装置からの接続認証要求に対して、認証装置に接続認証要求を代理に問い合わせ、その応答をあたかも１つの認証装置の応答であるかのように応答する代理認証装置あるいはプログラムを介在させることにより、利用者ＩＤと利用者に割り当てたネットワークアドレスとの対応表を作成することを特徴とするもの。

【請求項４】請求項１、２、３のコンピュータ網への接続認証において、接続認証要求を送出する相手を複数の接続認証装置の中から選びだすことを特徴とするもの。

【請求項５】請求項１、２、３のコンピュータ網への接続認証および履歴算出および記録装置、方法において、該機能を回線接続装置内に実現したことを特徴とするもの。

【請求項６】請求項１、２、３のコンピュータ網への接続認証および履歴算出および記録装置、方法において、該機能を経路制御装置内に実現したことを特徴とするもの。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、コンピュータ網の構成方法の１つであるダイヤルアップ通信における認証、接続履歴算出、記録、課金に関するものであり、特に、課金形態及び端末種別の多様化、端末数の大規模化に関する。

【０００２】

【従来の技術】図９に、ＲＦＣ２０５８、ＲＦＣ２０５９に基づいて動作する標準的な認証及び接続履歴装置の構成を示す。これらの装置は、ダイヤルアップによるコンピュータ網への接続時に、適正な利用者かどうかの認

2

証を行うことによって不正な接続を防止し（ＲＦＣ２０５８）、同時に、接続履歴を記録することによって、課金のためのデータを作成するもの（ＲＦＣ２０５９）である。回線接続装置０２には、１つ以上の接続用回線が用意されている。利用者は、この接続用回線を経由して、該コンピュータ網へと接続する。また、認証装置１４には、利用者ＩＤとそれに対応するパスワードの組が必要分記録されている。利用者は、回線接続装置０２への接続を試みる場合、自らの利用者ＩＤとパスワードの組を回線接続装置０２に対して送出する。回線接続装置０２は、利用者からの接続要求を検知すると、認証装置１４に対して、この情報の認証を要求する認証要求命令を送出する。認証装置１４は、認証要求命令を受け取ると、保有する利用者ＩＤとパスワードの組を走査し、認証の許可または不許可を決定する。認証装置１４は、許可の場合は接続許可応答を、不許可の場合は接続不許可応答を、回線接続装置０２に対して送出する。不許可の場合は、接続許可応答を返送しない事により代替する場合もある。回線接続装置０２は、認証装置より接続許可応答を受信すると、利用者の利用している回線におけるコンピュータ網への接続を開始する。これは、利用者側からコンピュータ網側へのパケットの転送、コンピュータ網側から利用者側へのパケットの転送といった一連の操作を指す。同時に、履歴記録装置１５に対して、利用者ＩＤを含んだ回線利用開始情報を送出する。接続が許可されなかった場合には、利用者の回線を切断する。回線接続装置０２は、利用者側からの回線切断を検知した場合などには、当該する回線を切断する。回線を切断する場合には、履歴記録装置１５に対して、利用者ＩＤ及び回線利用時間を含んだ回線利用終了情報を送出する。履歴記録装置１５は、回線利用開始情報あるいは回線利用終了情報を受信した場合、これらを通信履歴として記録する。履歴記録装置の出力の例を、図１２の上部に示す。

【０００３】

【発明が解決しようとする課題】しかしながら、上記のような従来のコンピュータ網接続認証方法や履歴記録方法では、利用者の回線接続時間や送受信データ量に基づいた課金のみが可能であり、通信回線の利用形態に基づいた多様な課金形態は可能ではなかった。利用形態に基づいた課金形態とは、たとえば、電子メールのみの利用であれば料金は無料であるが、Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂの利用であれば１分１０円を課金するといった課金や、符合化音声に対しては１分２０円を課金するといった課金や、接続している端末の種別によって基本料金が異なるなどの、利用形態毎に異なる料金表を適用する課金を指す。さらに、利用者の認証において、認証装置を静的に設定する必要があったために、実用的には利用者数に数万件程度の上限があった。

【０００４】

【課題を解決するための手段および発明の効果】そこで、本発明は、利用者ＩＤと割り当てネットワークアドレスとの対応表を作成することにより、コンピュータ網上のパケットの利用者を特定することを可能とする。また、パケットに含まれている情報のプロトコルを判別することによって、利用者ＩＤと利用しているプロトコルの組み合わせ毎に通信時間の履歴を算出し記録することを可能とする。また、請求項３の装置において、該対応表を作成する際に複数の認証装置の中から適切な認証装置を選択することによって、利用者認証の大規模化を可能とする。

【０００５】

【作用】請求項１の装置、あるいは請求項２の方法によって、利用者ＩＤと利用プロトコルの組み合わせ毎に通信を検知し、セッションの長さを計算し、通信履歴を記録することが可能となる。これらの通信履歴を利用することによって、利用形態に応じた課金を行うことが可能となる。

【０００６】請求項３の代理認証装置によって、既存の一般的なコンピュータ網接続認証装置や履歴記録装置の構成を変更することなく、本発明を利用することが可能となる。また、それらを極めて大規模に行うことが可能となる。

【０００７】本発明において、課金とは、記録されている通信履歴を料金表に照らして定められる概念であり、これらの装置そのものが課金を行うわけではない。

【０００８】本発明において、回線接続とは、利用者との間に物理的な接続、あるいは通信会社により提供されている仮想的な物理的回線接続を確立することを言う。また、コンピュータ網への接続とは、利用者が、コンピュータ網におけるパケット交換サービスを享受できる状態にすることを指す。

【０００９】本発明において、代理認証とは、認証要求を受信した際、他の認証装置に対してこの認証要求を転送し、受け取る応答をあたかも自らが認証したかのように認証要求に対して応答することを指す。

【００１０】本発明において、セッションとは、ある割り当てネットワークアドレスを利用した通信において、あるプロトコルを利用した最初のパケットの送出から、最後のパケットが送出されるまでの通信を指す。最後のパケットとは、パケット監視の精度として定められた時間を超えて通信が行われなかった場合の最後のパケットを指す事後的に成立するものとし、ＴＣＰのセッションとは異なった意味で用いる。図１０に、概念図を示す。

【００１１】

【発明の実施の形態】図１に、装置の全体構成を示す。これらの装置は、ハードウエアロジックによって構成することも、プログラムを用いてコンピュータ上に実装することもできる。また、プログラムを用いることで同一機器内に複数の機能を実現してもよい。

【００１２】図２に、実施例の動作概要を示す。回線接続装置０２は、利用者が該装置に接続するとき、利用者側端末より送出される利用者ＩＤとパスワードの組や利用者が利用している回線番号、割り当てネットワークアドレスなどの情報を、認証装置あるいは代理認証装置に送出し、認証要求を行う。回線接続装置は、モデムサーバやネットワークアクセスサーバといった呼称も有する。代理認証装置１１は、認証要求に含まれる情報より複数の認証装置の中から適当な認証装置を選択し、該利用者の認証を要求する。認証が行われた場合、該装置は利用者ＩＤと割り当てネットワークアドレスの組を対応表に記録した上で、回線接続装置０２に接続許可を与える。このように、代理認証装置１１は、回線接続装置０２側から見ると１つの認証装置であるかのように動作する。これらの操作を経ることによって、常に、割り当てネットワークアドレスと利用者ＩＤとの対応を把握することが可能となる。（図２Ｓ１）

認証装置１４は、回線接続装置０２や代理認証装置１１からの認証の要求に対して認証を行い、許可の場合は接続許可応答を、不許可の場合は接続不許可応答を、回線接続装置０２に対して送出する。不許可の場合は、接続許可応答を返送しない事により代替する場合もある。トラフィック監視装置１２は、このコンピュータの有するネットワークインターフェースを利用することによって、該装置が接続されたネットワーク・セグメント（図２Ｓ５）を監視し、割り当てネットワークアドレス宛および割り当てネットワークアドレスから送出されたパケットの情報を取得することができる。そこで、割り当てネットワークアドレスによる通信が行われ始めると、先の割り当てネットワークアドレスと利用者ＩＤの対応表から、それぞれの送受信パケットの利用者ＩＤを特定し、さらにパケット内の情報を解析する事により利用プロトコルを特定し、セッションタイマ装置１３に利用者ＩＤ、利用プロトコルを通知する。（図２Ｓ２）

セッションタイマ装置１３は、利用者ＩＤと利用プロトコルの組によって区別されるセッション毎にタイマを保有しており、セッションの通信時間を計測する。（図２Ｓ３）また、計測したセッションの通信履歴を、セッション開始情報及び終了情報を履歴記録装置に送出する。（図２Ｓ３）

図３にセッションタイマ装置の動作手順をフローチャートとして示す。セッションタイマ装置１３は、トラフィック監視装置１２からの通知があった際に、該当するセッションに対応するタイマを規定の値にリセットする。通知されたセッションに該当するタイマが起動していない場合には、タイマをセットした後に、セッション開始情報を履歴記録装置１５に送出する（図３Ｓ１）。タイマ機構は、一定期間毎に起動され、現在保有しているすべてのタイマに対し一定の減算を行う（図３Ｓ２）。タイムアウトした場合、すなわち、規定時間内に同一利用

5

者の該当するプロトコルの通信がなされなかった場合には、該当するセッションが終了したと見なし、履歴記録装置１５に対して該セッションの通信時間を記したセッション終了情報を送出し、タイマを削除する。、また、利用者の回線切断を検出した場合には、該利用者に属するセッションがすべて終了したものと見做し、履歴記録装置１５に対してすべてのセッションのセッション終了情報を送出する。（図３Ｓ３）

セッションの通信時間は、現在時刻よりタイマに記されているセッションの開始時刻及び規定のタイムアウトを減算することで算出できる。タイマによって管理されるデータの例を図１１に概念的に示す。なお、タイマの既定値は、別に設定データを保有するものとする。履歴記録装置１５は、回線接続装置０２やセッションタイマ装置１３などから、ある利用者における回線利用やセッションの開始および終了に関する情報を通知され、これらを記録する。本発明によって可能となる通信履歴の記録例を図１２下部に示す。各装置が以上のように連携し動作することによって、利用者が利用しているプロトコル毎に、通信履歴を記録することが可能となる。

【００１３】図４に、図１の代理認証装置１１、トラフィック監視装置１２、セッションタイマ装置１３を１つのコンピュータ内にプログラムとして実装した実施形態の構成を示す。

【００１４】図５に、図１の代理認証装置１１、トラフィック監視装置１２、セッションタイマ装置１３を経路制御装置内に実現した場合の構成を示す。経路制御装置０４内の経路制御機構は、該装置によって経路制御されるすべての通信内容を検出している必要がある。したがって、トラフィック監視装置１２を経路制御機構に包含することが可能となっている。

【００１５】図６に、図１の代理認証装置１１、トラフィック監視装置１２、セッションタイマ装置１２を回線接続装置内に実現した場合の構成を示す。回線接続装置０２は、利用者からのすべての通信内容を検出している必要がある。したがって、トラフィック監視装置１２を回線接続装置０２内の経路制御機構に包含することが可能となっている。

【００１６】上記の実施形態では、複数の認証装置を同一のネットワーク・セグメント上に設置しているが、図７に示すように、これらはコンピュータ網上に分散していてもよい。

【００１７】さらに、図８に示すように、コンピュータ網にインターネット・ファックスやインターネット電話といった機器の接続を試みる場合に、本発明による通信履歴を利用することによって、多様な課金形態を取ることも可能である。すなわち、機器種別毎に別々の料金表を適用することが可能となる。また、代理認証装置によって、機器毎に独立した認証を行い、かつ大規模化が可能となる。

6

【００１８】なお、各装置やプログラムが連携して動作する際の方法は、制御用のパケットを送受信することによっても、共有メモリやファイルの共有などの方法によって実現することも可能である。

【００２０】また、利用者への割り当てネットワークアドレスは、回線接続時に割り当てることも、予め割り当てておくこともできる。

【００２１】また、タイマの精度や認証装置の選択といった各装置の動作は、図中では省略した各種のパラメータによって規定されるものとする。

【００２２】また、上記実施形態では、複数の認証装置を利用しているが、単独の認証装置内に複数の認証機構を実装することによっても、同様の効果をあげることが可能である。

【００２３】また、複数の認証装置から特定の認証装置を選択する基準に関しては、利用者ＩＤの形式に依存させることで実現できる。たとえば、利用者ＩＤの１桁めによって認証装置を切り替えるなどである。

【図面の簡単な説明】

【図１】発明の全体構成を示す図。

【図２】発明の原理を示す図。

【図３】セッションタイマ装置のフローチャート。

【図４】図１の装置を、ネットワーク・セグメント監視機器内に実現した場合のシステム構成を示す図。

【図５】図１の装置を、経路制御装置内に実現した場合のシステム構成を示す図。

【図６】図１の装置を、回線接続装置内に実現した場合のシステム構成を示す図。

【図７】コンピュータ網上に分散した認証装置を利用するために本発明の利用した実施形態の構成を示す図。

【図８】インターネット・ファックスやインターネット電話などの機器別認証を行うために本発明を利用した実施形態の構成を示す図。

【図９】従来の認証／課金装置の構成を示す図。

【図１０】本発明におけるセッションの概念を示す図。

【図１１】本発明によるタイマ管理の例を示す図。

【図１２】従来の履歴記録と本発明によって可能となる通信履歴記録の例を示す図。

【符号の説明】

０１…ネットワーク・セグメント、０２…回線接続装置、０３…電話回線、０４…経路制御装置、０５…コンピュータ網、１１…代理認証装置、或いは、機構

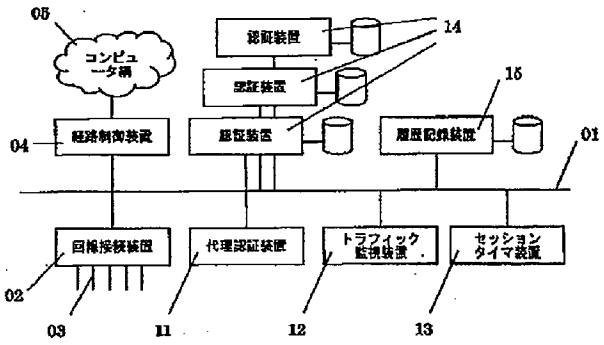
１２…トラフィック監視装置、或いは、機構

１３…セッションタイマ装置、或いは、機構

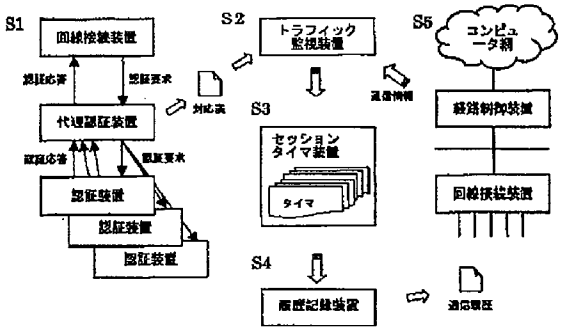
１４…認証装置、或いは、機構

１５…履歴記録装置

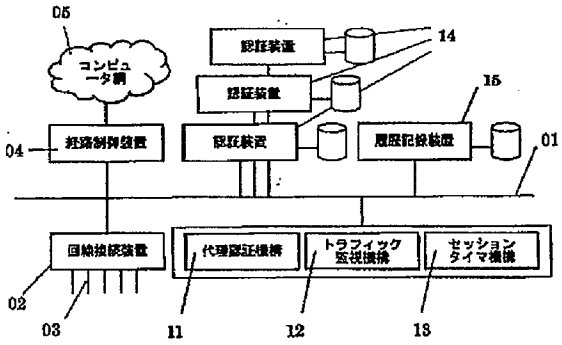
【図１】



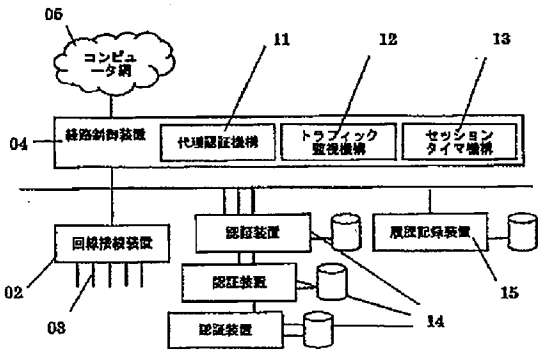
【図２】



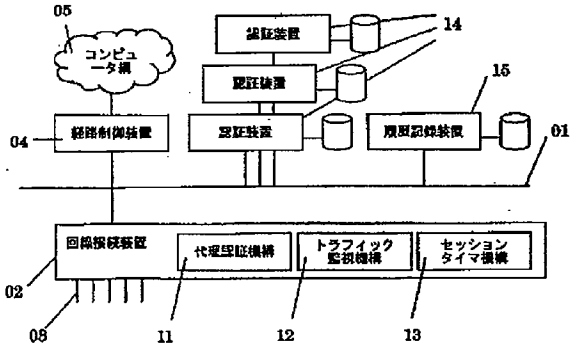
【図４】



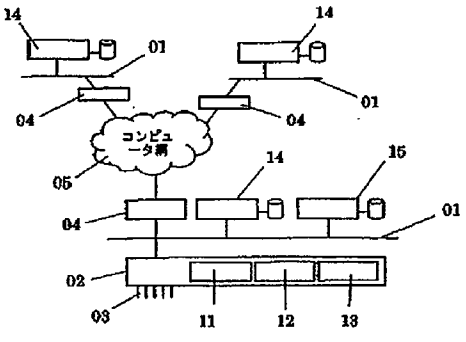
【図５】



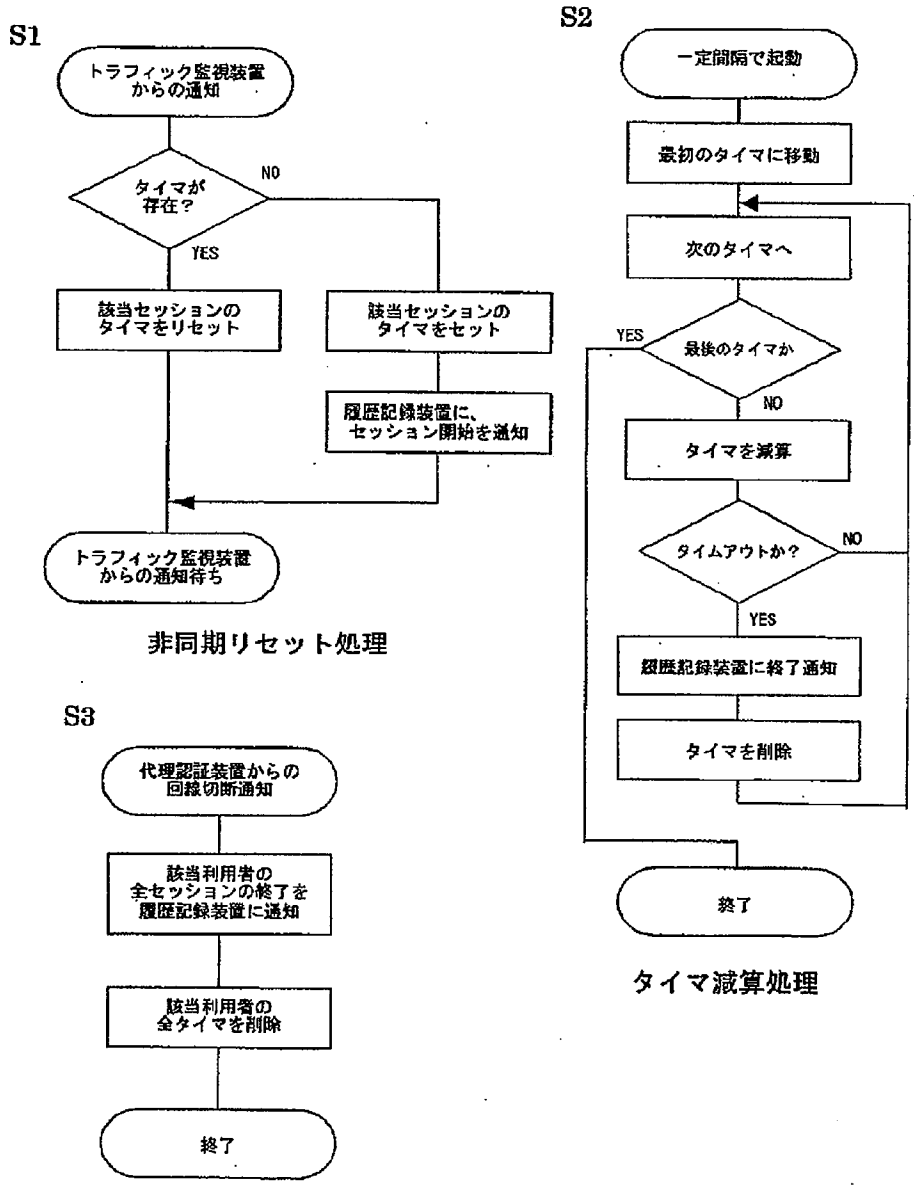
【図６】



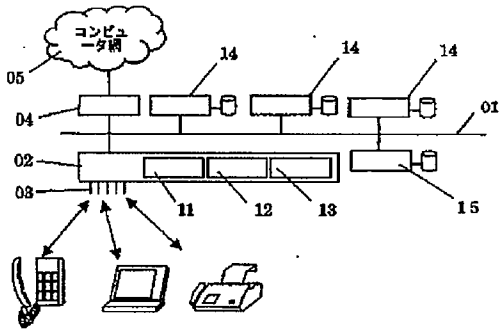
【図７】



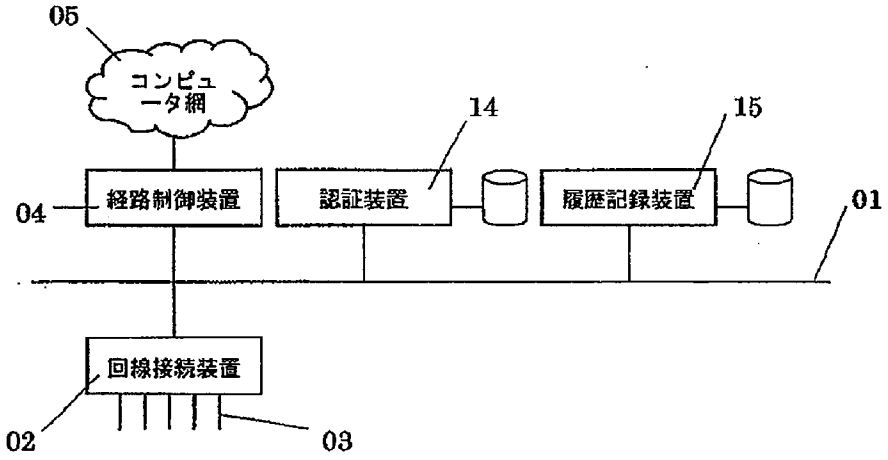
【図３】


S1
トラフィック監視装置からの通知
タイマが存在？
NO
YES
該当セッションのタイマをリセット
該当セッションのタイマをセット
履歴記録装置に、セッション開始を通知
トラフィック監視装置からの通知待ち
非同期リセット処理
S2
一定間隔で起動
最初のタイマに移動
次のタイマへ
YES
最後のタイマか
NO
タイマを減算
タイムアウトか？
NO
YES
履歴記録装置に終了通知
タイマを削除
終了
タイマ減算処理
S3
代理認証装置からの回線切断通知
該当利用者の全セッションの終了を履歴記録装置に通知
該当利用者の全タイマを削除
終了
回線切断処理

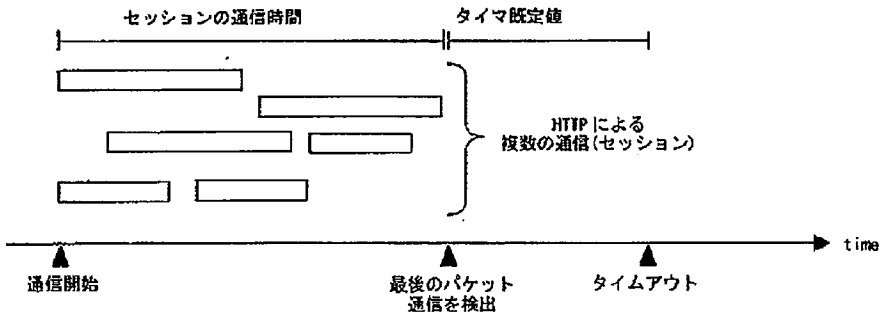
【図８】



【図９】



【図１０】



セッションの通信時間 ＝ タイムアウト時刻 － 開始時間 － タイマ既定値

セッションの通信時間の概念

【図１１】

利用者 ID	プロトコル	開始時間	タイマ
Hato	NNTP	1998/08/30 16:12:25	68
Taka	SMTP	1998/08/30 16:13:51	15
Taka	POP3	1998/08/30 16:15:41	42
Taka	HTTP	1998/08/30 16:13:05	32
Taost6	HTTP	1998/08/30 16:16:47	42
Taost6	POP3	1998/08/30 16:19:21	52

セッションタイマの概念図

【図１２】

記録時間	利用者 ID	履歴種別	通信時間
1998/08/30 16:08:23	利用者 Taka	接続開始	
1998/08/30 16:08:43	利用者 Hato	接続開始	
1998/08/30 16:09:36	利用者 Hato	接続終了	316
1998/08/30 16:10:03	利用者 Taka	接続終了	731
.			
.			

従来の履歴記録の例

記録時間	利用者 ID	履歴種別	プロトコル	通信時間
1998/08/30 16:08:23	利用者 Taka	接続開始		
1998/08/30 16:12:25	利用者 Taka	接続開始	TELNET	
1998/08/30 16:24:38	利用者 Taka	接続開始	POP3	
1998/08/30 16:29:03	利用者 Hato	接続開始		
1998/08/30 16:39:04	利用者 Hato	接続開始	HTTP	
1998/08/30 16:41:36	利用者 Taka	接続終了	POP3	901
1998/08/30 16:51:53	利用者 Hato	接続開始	TELNET	
1998/08/30 16:53:06	利用者 Taka	接続終了	TELNET	24
1998/08/30 16:54:43	利用者 Hato	接続終了	HTTP	453

本発明による履歴記録の例